AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for managing information retention in a system, comprising:

receiving a set of information into a system;

associating one or more keys with said set of information;

encrypting said set of information using said one or more keys;

storing said set of information in encrypted form into one or more repositories, wherein only the encrypted form of the set of information is persistently stored within the information system and no unencrypted form of the set of information is persistently stored within the information system; ~~and~~

purging said set of information from the system so that said set of information is not available ~~within~~ to a user from the system by deleting said one or more keys, thereby making said set of information unrenderable;

prior to deletion of said one or more keys, receiving a request from an information sink to render said set of information to a user;

accessing the encrypted form of said set of information from the one or more repositories;

accessing said one or more keys;

providing the encrypted form of said set of information and said one or more keys to the information sink to enable the information sink to decrypt the encrypted form of said set of information; and

using said one or more keys to render said set of information to the user, wherein the information sink comprises sufficient logic to prevent it from persistently storing said one or more keys received from an information manager.

2. (Original) The method of claim 1, wherein said set of information is purged from the system without requiring that the encrypted form of said set of information be deleted from the one or more repositories.

3. (Original) The method of claim 1, wherein said set of information is stored in the one or more repositories only in encrypted form.

4. (Original) The method of claim 1, wherein said one or more keys comprises a symmetrically paired set of keys.

5. (Original) The method of claim 1, further comprising:

prior to deletion of said one or more keys, receiving a request from an information sink to render said set of information to a user;

accessing the encrypted form of said set of information from the one or more repositories;

decrypting the encrypted form of said set of information using said one or more keys to derive said set of information; and

providing said set of information to the information sink to render said set of information to the user.

6. (Original) The method of claim 5, wherein said set of information is stored in the one or more repositories only in encrypted form, and wherein the encrypted form of said set of information is decrypted only when it is necessary to render said set of information to the user.

7 (Canceled).

8. (Currently amended) The method of ~~claim 7~~claim 1, wherein said set of information is stored in the one or more repositories only in encrypted form, and wherein the encrypted form of said set of information is decrypted only when it is necessary to render said set of information to the user.

9. (Original) The method of claim 1, wherein purging comprises:

determining, based upon an information retention policy, whether said set of information should be purged from the system; and

in response to a determination that said set of information should be purged from the system, purging said set of information from the system by deleting said one or more keys, thereby making said set of information unrenderable.

10. (Original) The method of claim 9, wherein said information retention policy is time-based such that said set of information is purged after a certain period of time.

11. (Original) The method of claim 9, wherein said information retention policy is condition-based such that said set of information is purged when one or more conditions are satisfied.

12. (Currently amended) An apparatus for managing information retention in a system, comprising:

a mechanism for receiving a set of information into a system;

a mechanism for associating one or more keys with said set of information;

a mechanism for encrypting said set of information using said one or more keys;

a mechanism for storing said set of information in encrypted form into one or more repositories, wherein only the encrypted form of the set of information is persistently stored within the information system and no unencrypted form of the set of information is persistently stored within the information system; ~~and~~

a mechanism for purging said set of information from the system so that said set of information is not available ~~within~~ to a user from the system by deleting said one or more keys, thereby making said set of information unrenderable;

a mechanism for receiving, prior to deletion of said one or more keys, a request from an information sink to render said set of information to a user;

a mechanism for accessing the encrypted form of said set of information from the one or more repositories;

a mechanism for accessing said one or more keys;

a mechanism for providing the encrypted form of said set of information and said one or more keys to the information sink to enable the information sink to decrypt the encrypted form of said set of information; and

using said one or more keys to render said set of information to the user, wherein the information sink comprises sufficient logic to prevent it from persistently storing said one or more keys received from an information manager.

13. (Original) The apparatus of claim 12, wherein said set of information is purged from the system without requiring that the encrypted form of said set of information be deleted from the one or more repositories.

14. (Original) The apparatus of claim 12, wherein said set of information is stored in the one or more repositories only in encrypted form.

15. (Original) The apparatus of claim 12, wherein said one or more keys comprises a symmetrically paired set of keys.

16. (Original) The apparatus of claim 12, further comprising:

a mechanism for receiving, prior to deletion of said one or more keys, a request from an information sink to render said set of information to a user;

a mechanism for accessing the encrypted form of said set of information from the one or more repositories;

a mechanism for decrypting the encrypted form of said set of information using said one or more keys to derive said set of information; and

a mechanism for providing said set of information to the information sink to enable the information sink to render said set of information to the user.

17. (Original) The apparatus of claim 16, wherein said set of information is stored in the one or more repositories only in encrypted form, and wherein the encrypted form of said set of information is decrypted only when it is necessary to render said set of information to the user.

18 (Canceled).

19. (Currently amended) The apparatus of ~~claim 18~~claim 12, wherein said set of information is stored in the one or more repositories only in encrypted form, and wherein the encrypted form of said set of information is decrypted by the information sink only when it is necessary to render said set of information to the user.

20. (Original) The apparatus of claim 12, wherein the mechanism for purging comprises:

a mechanism for determining, based upon an information retention policy, whether said set of information should be purged from the system; and

a mechanism for deleting, in response to a determination that said set of information should be purged from the system, said one or more keys, thereby making said set of information unrenderable.

21. (Original) The apparatus of claim 20, wherein said information retention policy is time-based such that said set of information is purged after a certain period of time.

22. (Original) The apparatus of claim 20, wherein said information retention policy is condition-based such that said set of information is purged when one or more conditions are satisfied.

23. (Currently amended) A computer readable medium having stored thereon instructions which, when executed by one or more processors, cause the one or more processors to manage information retention in a system, comprising:

instructions for causing one or more processors to receive a set of information into a system;

instructions for causing one or more processors to associate one or more keys with said set of information;

instructions for causing one or more processors to encrypt said set of information using said one or more keys;

instructions for causing one or more processors to store said set of information in encrypted form into one or more repositories;

wherein only the encrypted form of the set of information is persistently stored within the information system and no unencrypted form of the set of information is persistently stored within the information system, ~~and~~

instructions for causing one or more processors to purge said set of information from the system so that said set of information is not available ~~within~~ to a user from the system by deleting said one or more keys, thereby making said set of information unrenderable;

instructions for causing one or more processors to receive, prior to deletion of said one or more keys, a request from an information sink to render said set of information to a user;

instructions for causing one or more processors to access the encrypted form of said set of information from the one or more repositories;

instructions for causing one or more processors to access said one or more keys;

instructions for causing one or more processors to provide the encrypted form of said set of information and said one or more keys to the information sink to enable the information sink to decrypt the encrypted form of said set of information; and

instructions for using said one or more keys to render said set of information to the user, wherein the information sink comprises sufficient logic to prevent it from persistently storing said one or more keys received from an information manager.

24. (Original) The computer readable medium of claim 23, wherein said set of information is purged from the system without requiring that the encrypted form of said set of information be deleted from the one or more repositories.

25. (Original) The computer readable medium of claim 23, wherein said set of information is stored in the one or more repositories only in encrypted form.

26. (Original) The computer readable medium of claim 23, wherein said one or more keys comprises a symmetrically paired set of keys.

27. (Original) The computer readable medium of claim 23, further comprising:

instructions for causing one or more processors to receive, prior to deletion of said one or more keys, a request from an information sink to render said set of information to a user;

instructions for causing one or more processors to access the encrypted form of said set of information from the one or more repositories;

instructions for causing one or more processors to decrypt the encrypted form of said set of information using said one or more keys to derive said set of information; and

instructions for causing one or more processors to provide said set of information to the information sink to enable the information sink to render said set of information to the user.

28. (Original) The computer readable medium of claim 27, wherein said set of information is stored in the one or more repositories only in encrypted form, and wherein the encrypted form of said set of information is decrypted only when it is necessary to render said set of information to the user.

29 (Canceled).

30. (Currently amended) The computer readable medium of ~~claim 29~~claim 23, wherein said set of information is stored in the one or more repositories only in encrypted form, and wherein the encrypted form of said set of information is

decrypted by the information sink only when it is necessary to render said set of information to the user.

31. (Original) The computer readable medium of claim 23, wherein the instructions for causing one or more processors to purge said set of information from the system comprises:

instructions for causing one or more processors to determine, based upon an information retention policy, whether said set of information should be purged from the system; and

instructions for causing one or more processors to delete, in response to a determination that said set of information should be purged from the system, said one or more keys, thereby making said set of information unrenderable.

32. (Original) The computer readable medium of claim 31, wherein said information retention policy is time-based such that said set of information is purged after a certain period of time.

33. (Original) The computer readable medium of claim 31, wherein said information retention policy is condition-based such that said set of information is purged when one or more conditions are satisfied.